FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1217765-0

Total Deleted Page(s) = 5
Page 8 ~ b7E;
Page 10 ~ b7E;
Page 11 ~ b7E;
Page 24 ~ b7E;
Page 26 ~ b7E;

```
XXXXXXXXXXXXXXXXXXXXXXXX
X   Deleted Page(s)    X
X   No Duplication Fee X
X   For this Page      X
XXXXXXXXXXXXXXXXXXXXXXXX
```

U.S. Cyber Threats

The Cyber Landscape

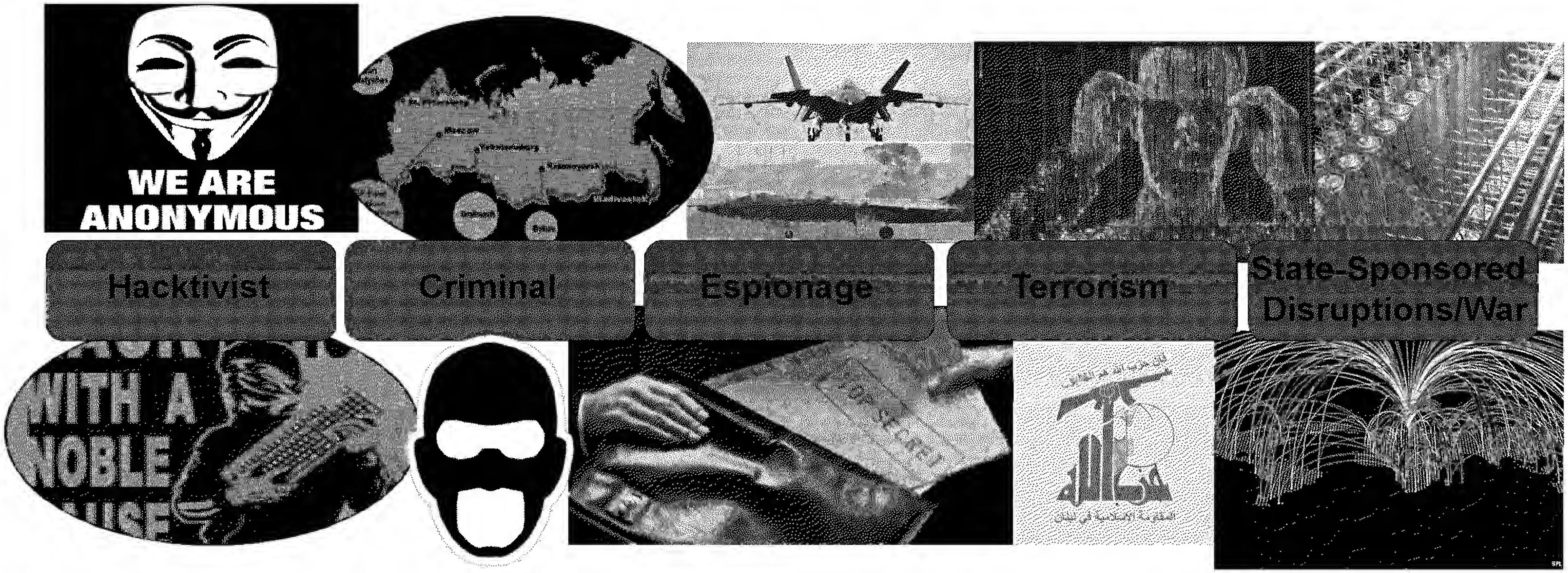
ASAC [redacted]

b6
b7C

FBI-Minneapolis Division

Minnesota Cyber Crime Task Force

U.S. Cyber Threats



Hacktivist

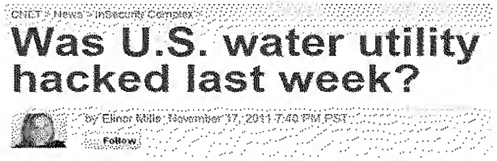
Criminal

Espionage

Terrorism

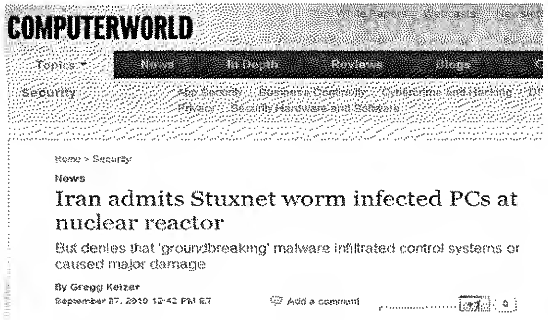
State-Sponsored Disruptions/War

Why the Computer Intrusion Priority?



Was U.S. water utility hacked last week?

by Elinor Mills November 17, 2011 7:40 PM PST

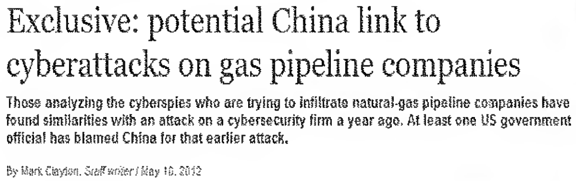


News

Iran admits Stuxnet worm infected PCs at nuclear reactor

But denies that 'groundbreaking' malware infiltrated control systems or caused major damage

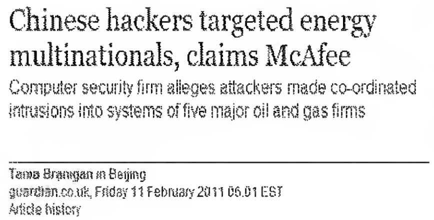
By Gregg Keizer
September 27, 2010 12:42 PM ET



Exclusive: potential China link to cyberattacks on gas pipeline companies

Those analyzing the cyberspies who are trying to infiltrate natural-gas pipeline companies have found similarities with an attack on a cybersecurity firm a year ago. At least one US government official has blamed China for that earlier attack.

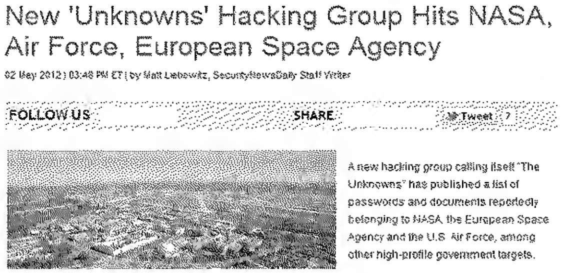
By Mark Clayton, *Staff writer* / May 10, 2012



Chinese hackers targeted energy multinationals, claims McAfee

Computer security firm alleges attackers made co-ordinated intrusions into systems of five major oil and gas firms

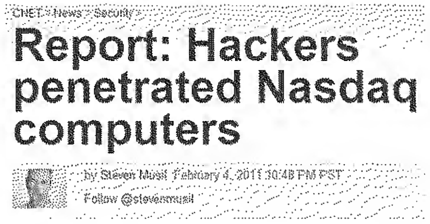
Tania Branigan in Beijing
guardian.co.uk, Friday 11 February 2011 06.01 EST
Article history



New 'Unknowns' Hacking Group Hits NASA, Air Force, European Space Agency

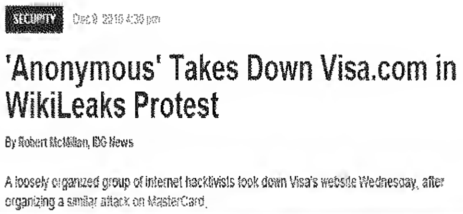
02 May 2012 | 03:48 PM ET | by Matt Liebowitz, SecurityNewsDaily Staff Writer

A new hacking group calling itself "The Unknowns" has published a list of passwords and documents reportedly belonging to NASA, the European Space Agency and the U.S. Air Force, among other high-profile government targets.



Report: Hackers penetrated Nasdaq computers

by Steven Musil February 4, 2011 10:48 PM PST
Follow @stevenmusil

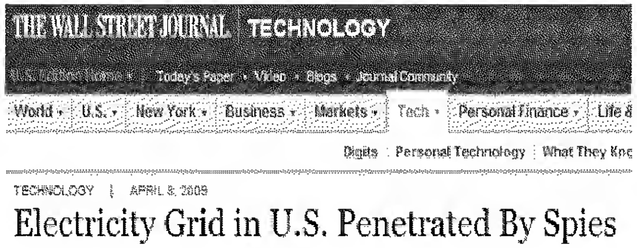


Dec 8, 2010 4:30 pm

'Anonymous' Takes Down Visa.com in WikiLeaks Protest

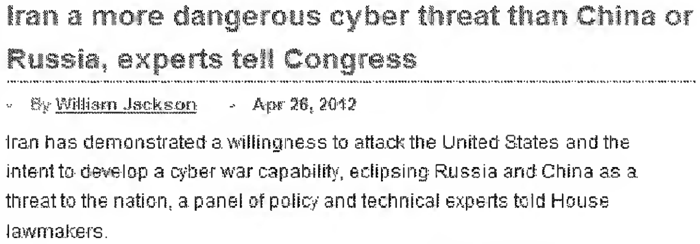
By Robert McMillan, IDG News

A loosely organized group of internet hacktivists took down Visa's website Wednesday, after organizing a similar attack on MasterCard.



TECHNOLOGY | APRIL 8, 2009

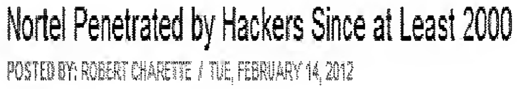
Electricity Grid in U.S. Penetrated By Spies



Iran a more dangerous cyber threat than China or Russia, experts tell Congress

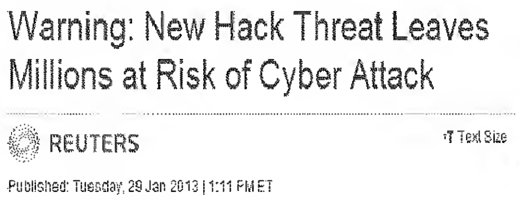
By William Jackson · Apr 26, 2012

Iran has demonstrated a willingness to attack the United States and the intent to develop a cyber war capability, eclipsing Russia and China as a threat to the nation, a panel of policy and technical experts told House lawmakers.



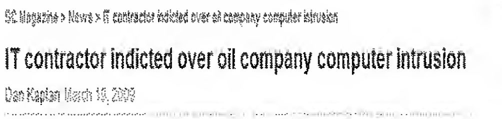
Nortel Penetrated by Hackers Since at Least 2000

POSTED BY: ROBERT CHARETTE / TUE, FEBRUARY 14, 2012



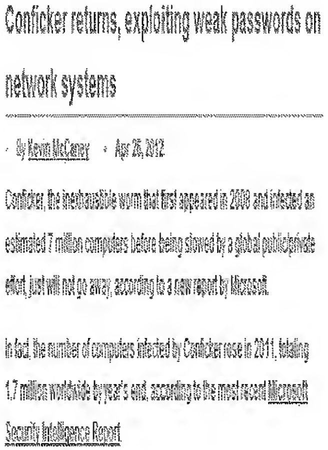
Warning: New Hack Threat Leaves Millions at Risk of Cyber Attack

Published: Tuesday, 29 Jan 2013 | 1:11 PM ET


SC Magazine > News > IT contractor indicted over oil company computer intrusion

IT contractor indicted over oil company computer intrusion

Dan Kaplan March 18, 2009

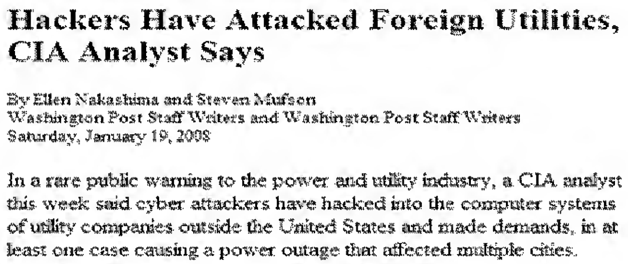


Conficker returns, exploiting weak passwords on network systems

By Kevin McCaney · Apr 26, 2012

Conficker, the inextinguishable worm that first appeared in 2008 and infected an estimated 7 million computers before being slowed by a global public/private effort, just will not go away, according to a new report by Microsoft.

In fact, the number of computers infected by Conficker rose in 2011, totaling 1.7 million worldwide by year's end, according to the most recent Microsoft Security Intelligence Report.

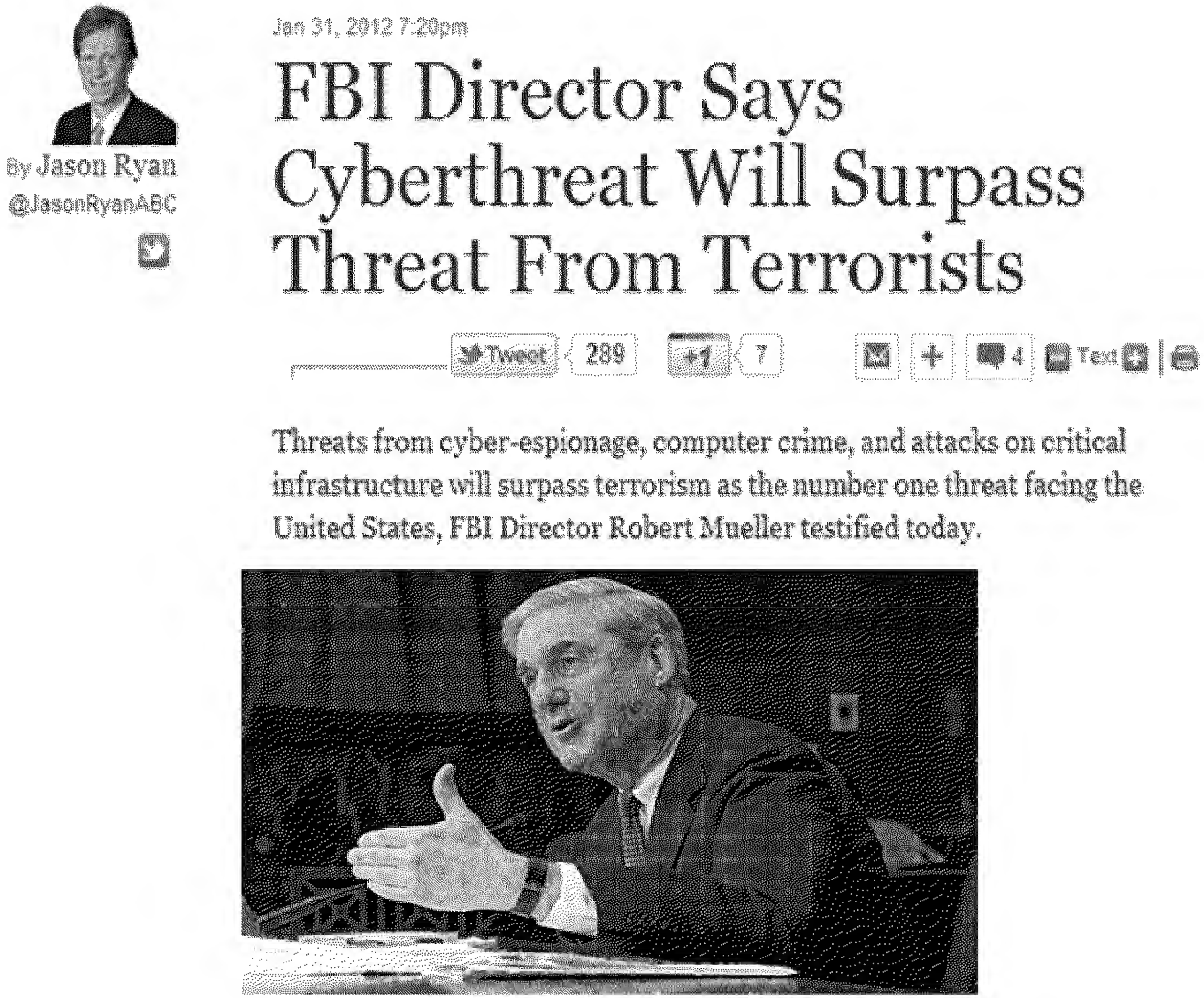


Hackers Have Attacked Foreign Utilities, CIA Analyst Says

By Ellen Nakashima and Steven Mufson
Washington Post Staff Writers and Washington Post Staff Writers
Saturday, January 19, 2008

In a rare public warning to the power and utility industry, a CIA analyst this week said cyber attackers have hacked into the computer systems of utility companies outside the United States and made demands, in at least one case causing a power outage that affected multiple cities.

FBI Cyber Priorities



By Jason Ryan
@JasonRyanABC

Jan 31, 2012 7:20pm

FBI Director Says Cyberthreat Will Surpass Threat From Terrorists

Threats from cyber-espionage, computer crime, and attacks on critical infrastructure will surpass terrorism as the number one threat facing the United States, FBI Director Robert Mueller testified today.

FBI Priorities

1. Protect the United States from terrorist attack.
2. Protect the United States against foreign intelligence operations and espionage.
3. **Protect the United States against cyber-based attacks and high-technology crimes.**
4. Combat public corruption at all levels.
5. Protect civil rights.
6. Combat transnational and national criminal organizations and enterprises.
7. Combat major white-collar crime.
8. Combat significant violent crime.
9. Support federal, state, county, municipal, and international partners.
10. Upgrade technology to successfully perform the FBI's mission.

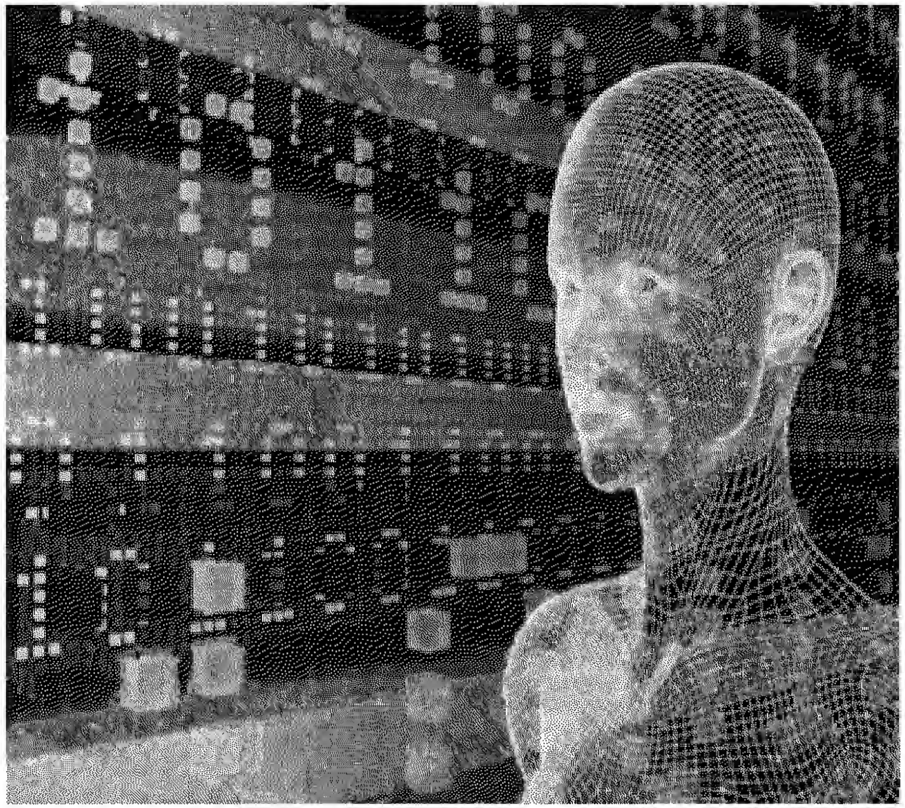
The Costs and Statistics

- Average time to resolve a cyber attack – 24 days
- Average cost to organizations of $591,780 over this 24 day period.
- 102 attacks per week on average
- Malware incidents – Significantly Affected 67.1% of organizations (trending upward)
- Botnet infections – 28.9% (trending upward)
- Theft of laptops – 33.5% (slight downward trend)

CSI 15th Annual 2010/2011 Computer Crime & Security Survey
Ponemon Institute (Third Annual) 2012 Cost of Cyber Crime Study: *United States*

Cyber Threat Investigation

Cyber Threat Investigation (n): "Any action taken within the United States, consistent with applicable law and Presidential guidance, to determine the identity, location, intent, motivation, capabilities, alliances, funding, or other methodologies of one or more cyber threat groups or individuals."



CTI and Net Defender Missions

Cyber Threat Investigation

- Understand & neutralize threat infrastructure
- Identify Victims
- Attribute threat actors & organizations
- Pursue actors & organizations

Computer Network Defense

- Prepare for attacks & reduce vulnerabilities
- Detect & analyze computer intrusions
- Learn from vulnerabilities exploited
- Manage and contain losses

U.S. Cyber Threats

Hacktivist | Criminal | Espionage | Terrorism | State-Sponsored Disruptions/War

Exclusive Title 18 Authority

Availability of Title 18 Authority

Title 50 Authority

Title 10 Military Authority

Hacktivist

Although the term “hacktivist” refers to cyber attacks conducted in the name of political activism, this segment of the cyber threat spectrum covers everything from individual hackers seeking thrills and bragging rights to hacker groups such as Anonymous and Lulz Security (LulzSec) conducting distributed denial of service (DDoS) attacks and website defacements against government. corporate entities.

rootkit phishing malware worm trojan virus spam hackers spyware security

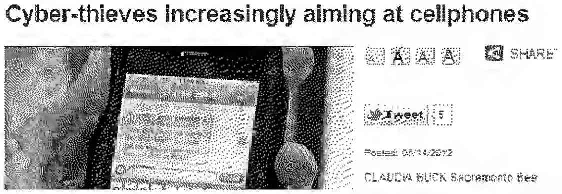
Criminal

Organized criminal groups have easily adapted to today’s technology in exploiting the cyber arena. These groups continually attack systems for monetary gain through identify theft, online fraud, computer extortion, phishing, and spyware/malware.

Criminal Acts

- Laptop Theft
- Credit Card Theft
- Telecom Fraud
- Financial Fraud
- Web Site Defacement
- Denial of Service
- Unauthorized Access
- Viruses
- Insider Abuse

- System Penetration
- Sabotage
- Mobile Device Hacking
- Abuse of Wireless Networks
- Bots
- Phishing Scams
- Social Engineering
- * Exploiting Social Networks
- E-commerce



Cyber-thieves increasingly aiming at cellphones

Posted: 05/14/2012

CLAUDIA BUCK Sacramento Bee

Cyber criminals are mass producing techniques, says Verizon

Targeting small-to-medium businesses

By **Lee Bell**

Thu May 10 2012, 17:00

CYBER CRIMINALS are mass producing their attack techniques and targeting smaller businesses, telecom Verizon has warned.

MAY 10, 2012

APT attackers are increasingly using booby -trapped RTF documents

Security experts say Microsoft Officer RTF parsing vulnerabilities are a common target for attackers who distribute advanced persistent threats

By Lucian Constantin , IDG News Service

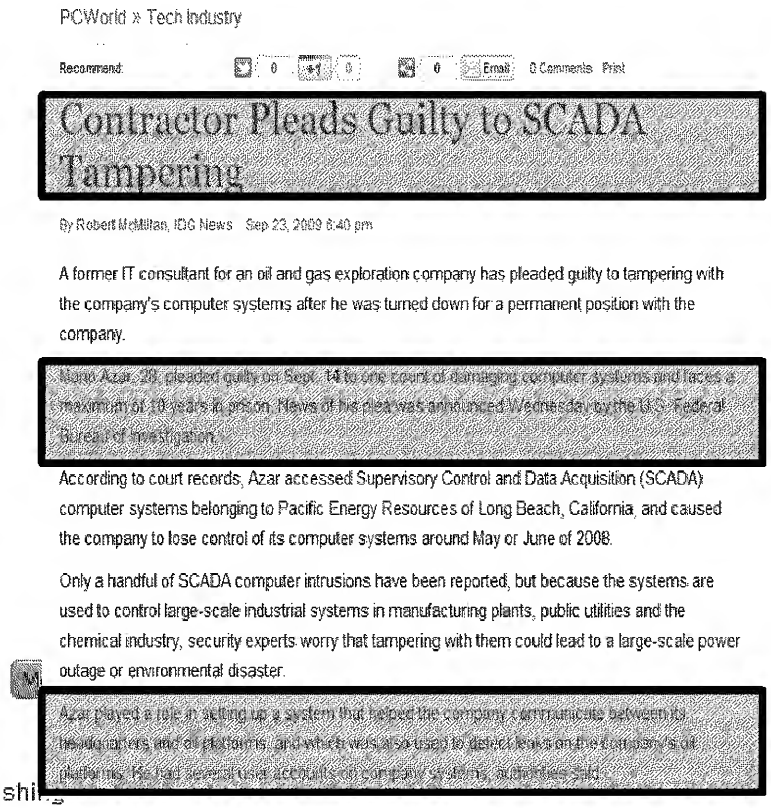
Cyber-criminals catch on to online hotel booking craze

14.05.2012

Categories: Consumer Tech, Internet, Software

Intentional or not, the end result is damage to your organization

- Disgruntled employees
- Excessive Access
- Inadvertent actions



Contractor Pleads Guilty to SCADA Tampering

By Robert McMillan, IDG News Sep 23, 2009 6:40 pm

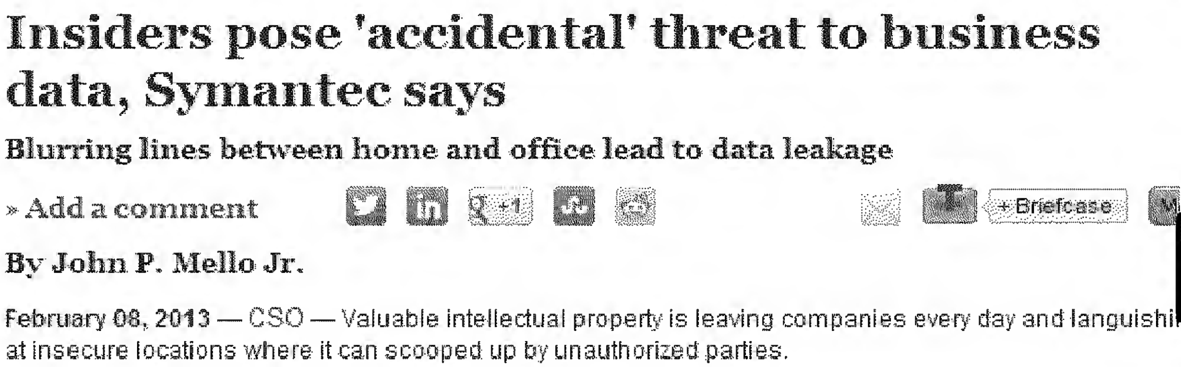
A former IT consultant for an oil and gas exploration company has pleaded guilty to tampering with the company's computer systems after he was turned down for a permanent position with the company.

Mario Azar, 28, pleaded guilty on Sept. 14 to one count of damaging computer systems and faces a maximum of 10 years in prison. News of his plea was announced Wednesday by the U.S. Federal Bureau of Investigation.

According to court records, Azar accessed Supervisory Control and Data Acquisition (SCADA) computer systems belonging to Pacific Energy Resources of Long Beach, California, and caused the company to lose control of its computer systems around May or June of 2008.

Only a handful of SCADA computer intrusions have been reported, but because the systems are used to control large-scale industrial systems in manufacturing plants, public utilities and the chemical industry, security experts worry that tampering with them could lead to a large-scale power outage or environmental disaster.

Azar played a role in setting up a system that helped the company communicate between its headquarters and oil platforms, and which was also used to detect leaks on the company's oil platforms. He had several user accounts on company systems, authorities said.



Insiders pose 'accidental' threat to business data, Symantec says

Blurring lines between home and office lead to data leakage

By John P. Mello Jr.

February 08, 2013 — CSO — Valuable intellectual property is leaving companies every day and languishi at insecure locations where it can scooped up by unauthorized parties.

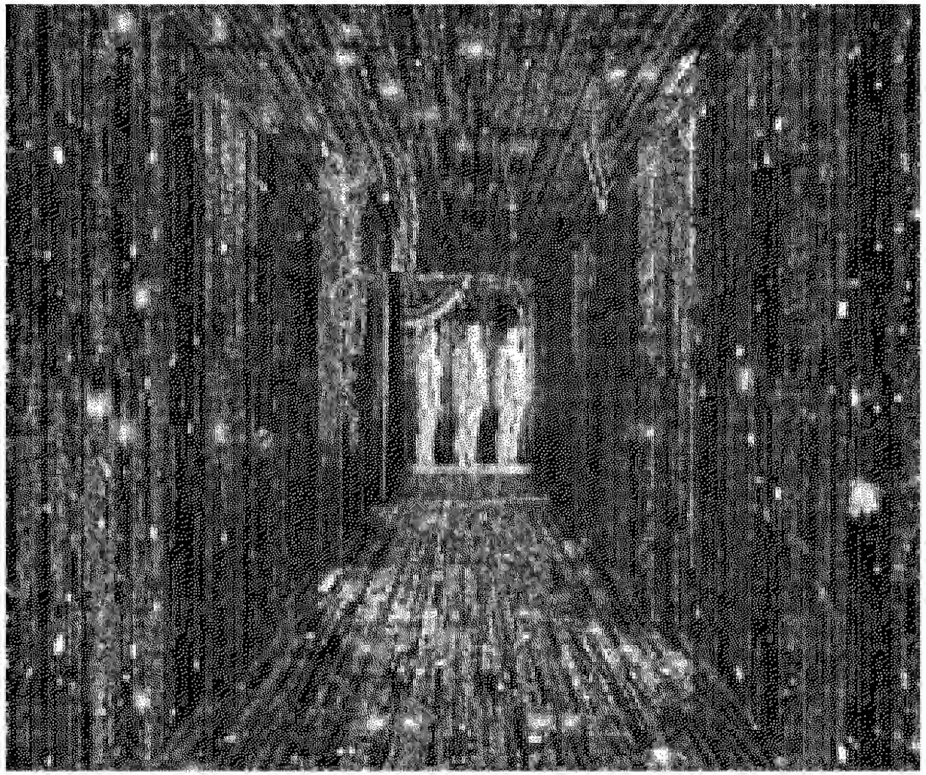
Industrial Espionage

Every year, billions of dollars are lost to foreign and domestic competitors who deliberately target economic intelligence in U.S. industries and technologies. Through cyber intrusions, these intruders search for intellectual property, prototypes, and company trade secrets to gain an illegitimate advantage in the market.

Reasons Why They'd Want to:

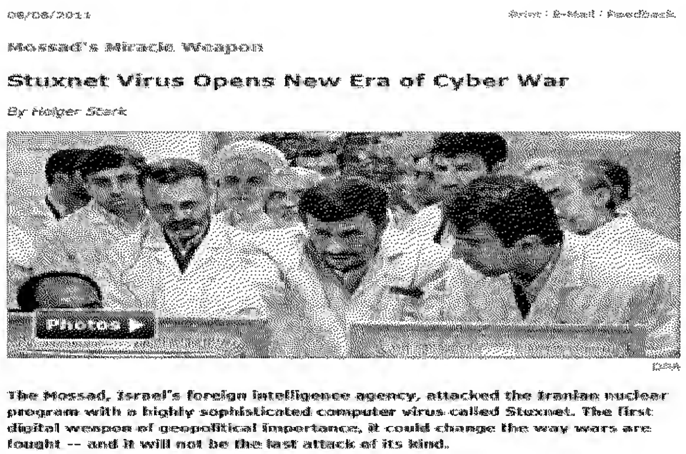
Steal Customer Lists
Steal R&D
Cause Bad PR
Disrupt Business
Sabotage

State Espionage



Foreign adversaries use cyber tools as part of traditional intelligence-gathering and espionage activities. These adversaries conduct computer network operations that target military and governmental organizations' intellectual property and insider information.

Foreign Powers



08/08/2011 Print | E-Mail | Feedback

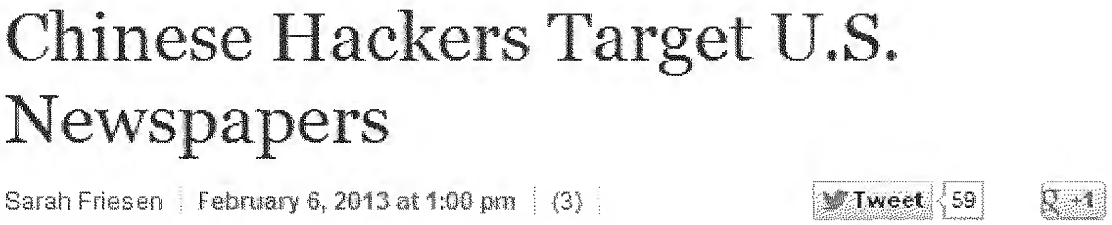
Mossad's Miracle Weapon

Stuxnet Virus Opens New Era of Cyber War

By Holger Stark

DPA

The Mossad, Israel's foreign intelligence agency, attacked the Iranian nuclear program with a highly sophisticated computer virus called Stuxnet. The first digital weapon of geopolitical importance, it could change the way wars are fought -- and it will not be the last attack of its kind.



Chinese Hackers Target U.S. Newspapers

Sarah Friesen | February 6, 2013 at 1:00 pm | (3)

Chinese hackers targeted energy multinationals, claims McAfee

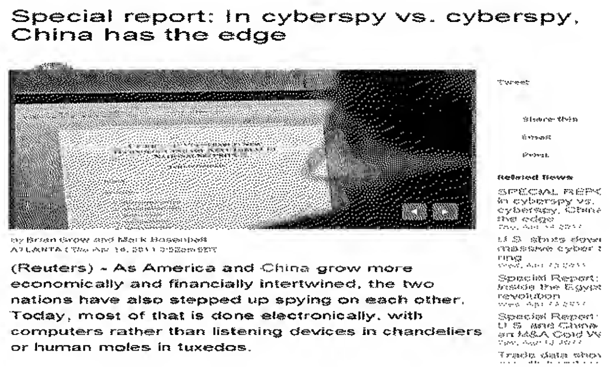
Computer security firm alleges attackers made co-ordinated intrusions into systems of five major oil and gas firms

Tania Branigan in Beijing
guardian.co.uk, Friday 11 February 2011 06.01 EST
Article history

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units



Special report: In cyberspy vs. cyberspy, China has the edge

By Brian Grow and Mark Hosenball
ATLANTA | Thu Apr 14, 2011 3:52pm EDT

(Reuters) - As America and China grow more economically and financially intertwined, the two nations have also stepped up spying on each other. Today, most of that is done electronically, with computers rather than listening devices in chandeliers or human moles in tuxedos.

Tweet
Share this
Email
Print
Related News
SPECIAL REPC in cyberspy vs. cyberspy, Chine the edge
U.S. shuts dowr massive cyber t ring
Special Report: Inside the Egypt revolution
Special Report: U.S. and China an M&A Cold W
Trade data show

THE WALL STREET JOURNAL | TECHNOLOGY
U.S. Edition Home • Today's Paper • Video • Blogs • Journal Community
World ▾ U.S. ▾ New York ▾ Business ▾ Markets ▾ Tech ▾ Personal Finance ▾ Life &
Digits | Personal Technology | What They Knc

TECHNOLOGY | APRIL 8, 2009

Electricity Grid in U.S. Penetrated By Spies

By Jason Ryan
@JasonRyanABC

Nov 3, 2011 1:22pm

US Official Singles Out China, Russia on Cyber-Spying

Mandiant Report

(Released February 2013)

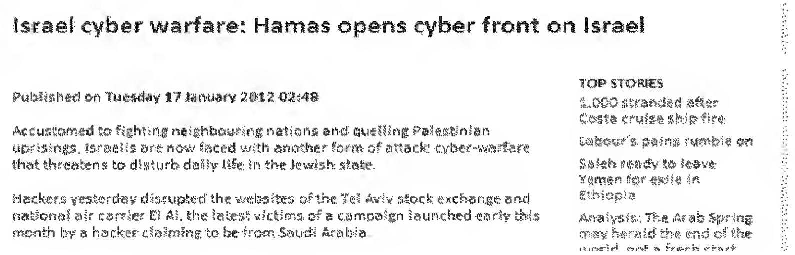
- Various cyber actors have engaged in malicious activity against Government and Private Sector entities
- The objective of this activity has been the theft of intellectual property, trade secrets, and other sensitive business information.
- The malicious actors have employed a variety of techniques in order to infiltrate targeted organizations, establish a foothold; move laterally through the targets' networks; and, exfiltrate confidential or proprietary data.

Industries Compromised - Mandiant

- Information Technology
- Aerospace
- Public Administration
- Satellites and Telecommunications
- Scientific Research and Consulting
- Energy
- Transportation
- Construction and Manufacturing
- Engineering Services
- High-tech Electronics
- International Organizations
- Legal Services
- Media, Advertising and Entertainment
- Navigation
- Chemicals
- Financial Services
- Food and Agriculture
- Healthcare
- Metals and Mining
- Education

targets at the direction, on behalf, or in support of a terrorist group or their ideology, through the use of computer network attack or exploitation. Such intrusions/attacks are intended to intimidate or coerce a government or population in furtherance of a social, political, ideological, or religious agenda by causing disruption, inducing fear, or undermining confidence.

Terrorists on the Internet



Israel cyber warfare: Hamas opens cyber front on Israel

Published on Tuesday 17 January 2012 02:48

Accustomed to fighting neighbouring nations and quelling Palestinian uprisings, Israelis are now faced with another form of attack: cyber-warfare that threatens to disturb daily life in the Jewish state.

Hackers yesterday disrupted the websites of the Tel Aviv stock exchange and national air carrier El Al, the latest victims of a campaign launched early this month by a hacker claiming to be from Saudi Arabia.

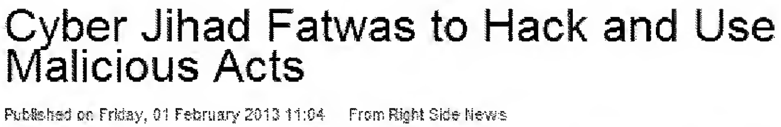
TOP STORIES

1,000 stranded after Costa cruise ship fire

Labour's pains rumble on

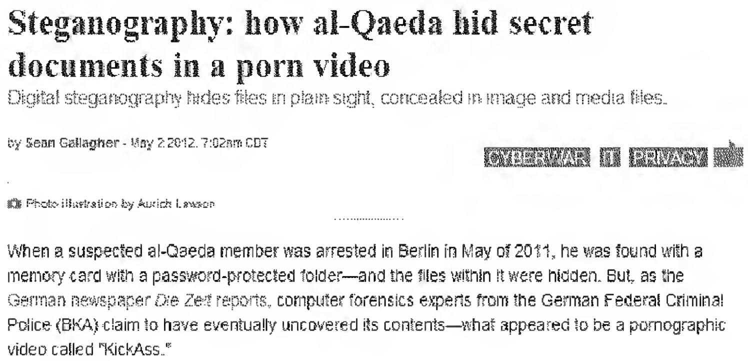
Saleh ready to leave Yemen for exile in Ethiopia

Analysis: The Arab Spring may herald the end of the



Cyber Jihad Fatwas to Hack and Use Malicious Acts

Published on Friday, 01 February 2013 11:04 From Right Side News



Steganography: how al-Qaeda hid secret documents in a porn video

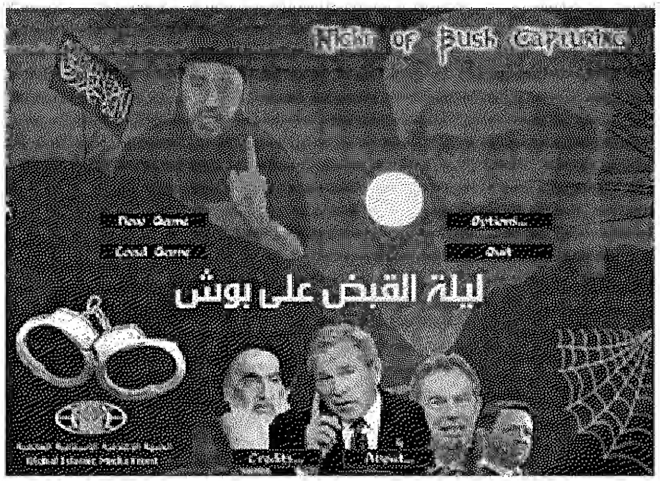
Digital steganography hides files in plain sight, concealed in image and media files.

by Sean Gallagher - May 2 2012, 7:02am CDT

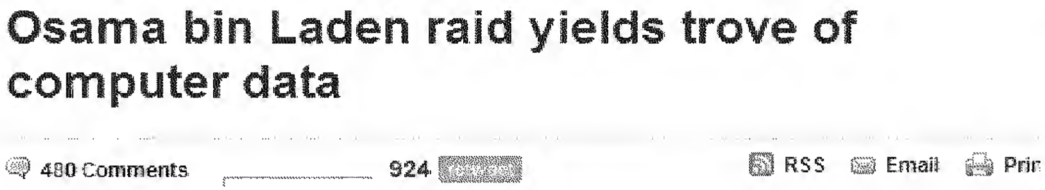
CYBERWAR IT PRIVACY

Photo illustration by Aurich Lawson

When a suspected al-Qaeda member was arrested in Berlin in May of 2011, he was found with a memory card with a password-protected folder—and the files within it were hidden. But, as the German newspaper *Die Zeit* reports, computer forensics experts from the German Federal Criminal Police (BKA) claim to have eventually uncovered its contents—what appeared to be a pornographic video called "KickAss."



One of the Global Islamic Media Front's most popular products was a videogame called *The Night of Bush Capturing*, the object of which is to hunt and kill the President of the United States.



Osama bin Laden raid yields trove of computer data

480 Comments 924 RSS Email Prir

What Can I Do?

- Implement strong passwords
- Limit the use of Privileged (Admin) Accounts
- Protect personal/business information
- Use caution with social networking sites
- **Use caution with email attachments and untrusted links**
- Apply Software Updates and Enable Future Automatic Updates

Where Can I Learn More?

- www.fbi.gov

iC3
INTERNET CRIME COMPLAINT CENTER

- www.us-cert.gov

U.S. DEPARTMENT OF HOMELAND SECURITY
US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

- www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf

IAD

Resources at: www.fbi.gov

Thank you for your attention!

ASAC [redacted]

b6
b7C

FBI-Minneapolis Division
Minnesota Cyber Crime Task Force
(763) 569-8000